图书情报工作
第63卷 第23期 2019年12月

移动互联网环境下用户账号注销机制研究*

吴任力[1] 吴淑倩[2]
[1] 武汉大学信息管理学院 武汉 430072 [2] 香港中文大学商学院 香港 999077

摘要：［目的/意义］在移动互联网环境下，手机应用（APP）服务商掌握了越来越多的用户数据，注销账号成为用户防止个人信息遭受非法利用的有效手段，账号注销机制的构建对保障用户信息安全具有重要意义。［方法/过程］在系统调查我国有关法律规定及欧盟 GDPR 法案的基础上，对国内外主流 APP 的账号注销机制进行全面梳理，分析其中存在的问题，并提出可行的建设策略。［结果/结论］提出在覆盖注销前、注销中、注销后三个阶段，由服务商、监管机构和用户三方协作参与的全流程账号注销机制，并指出了面向用户信息安全的管理与服务未来突破与创新的方向。

关键词：被遗忘权 个人数据 信息保护 数据删除 隐私影响评估
分类号：G203
DOI：10.13266/j.issn.0252-3116.2019.23.007

1 引言

在移动互联网时代，智能终端数量的激增使各类APP深入到大众生活的方方面面，用户隐私数据的爆发式增长也使在信息世界精准刻画和识别用户实体成为可能[1]。如今社交类 APP 的实名认证制度将用户真实的社交网络映射到虚拟空间；金融类 APP 通过身份证、银行卡的绑定掌握了用户的身份及经济信息；共享类 APP 允许用户公开更多数据及隐私以换取便利的服务[2]等。APP 服务商获取的数据已不再局限于用户主动提供的信息，诸如出行路程、浏览历史、个人偏好等用户在使用中形成的信息也被充分获取和使用。用户对个人隐私的让渡也带来了严峻的信息保护问题。2018年3月，百度 CEO 李彦宏在“中国发展论坛”发表的“中国用户愿用隐私换便利”的言论[3]引发轩然大波，随后京东利用用户消费数据“杀熟”的事件[4]也引发了公众的广泛关注。这些事件暴露出用户数据拥有者在数据处置中缺乏透明度的现实问题，反映了互联网用户在隐私保护中的无奈。

这些问题逐渐受到社会重视，调查发现民众对APP 隐私保护问题存在普遍担忧，并对用户的使用行为产生了巨大影响[5-7]。而账号注销作为个人信息退出的基本方案，是大数据和互联网环境下应对信息滥用、规避数据风险、加强安全管理的有效途径之一，已得到国际社会广泛关注。国外不但有专门评估 APP 账号删除难度的网站[8]，同时相关研究[9-11]认为允许用户删除账号是控制个人数据的重要措施，尤其在不再使用相关服务[12]和“数字死亡”[13]的情况下。此外2018年5月正式生效的欧盟《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）[14]所涉及的“擦除权”“数据可携带权”等数据主体权利，更是为账号注销奠定了法律基础，具有重要指导意义[15]。

我国用户账号注销的有关政策和实践尚待完善，立法工作的迟缓不但让 APP 服务商“滥用免责”，同时也使黑色产业链有机可乘。根据中国消费者协会2018年底发布的隐私报告显示[16]，在调研的100款APP 中，有70款未明确告知用户个人信息的保存期限，96款未明确告知用户如何撤回个人信息的授权同意。“账号注销难”问题日渐凸显，注销无门导致数据的无限期留存已成为威胁个人信息安全的巨大隐患。2018年初针对支付宝、百度等 APP 存在的侵犯用户隐私问题，工业和信息化部信息通信管理局约谈了相关单位，并指出将加强对“账户注销”环节的监督检

* 本文系国家知识产权局软科学研究项目“大数据产权安排及其制度构建路径”（项目编号：SS18-A-17）研究成果之一。
作者简介：吴任力（ORCID：0000-0003-2370-6236），硕士研究生，E-mail：wurenli@yeah.net；吴淑倩（ORCID：0000-0003-1896-6471），硕士研究生。
收稿日期：2019-02-10 修回日期：2019-05-21 本文起止页码：52-64 本文责任编辑：杜杏叶

查[17],同月在回应网民反映的 APP 销户问题时,工信部明确表示依据相关法律规定,用户有权删除在平台服务商注册的账户服务[18],并在去年多次就相关问题要求相关企业整改[19],这显示了我国政府惩治数据处理和保留“霸王条款”、保障用户注销权利的决心。

当前,有关用户账号注销的专门研究还较少。国外相关主题主要伴随隐私数据处理的研究出现,D. Herrmann 和 J. Lindemann[11]统计了德国境内上百个 APP 和流行网站对用户数据获取和删除请求的处理情况,证实其中只有一半调查对象给出了满意答复,不到六成能彻底清除用户数据;T. Antignac 等[20]设计了一种隐私概念模型用于处理个人数据,并将擦除个人数据作为保留期满后的重要环节。国外研究还对 APP 的隐私保护策略给予了较多关注,K. Fawaz 和 K. G. Shin[21]提出了应用于智能手机 APP 中位置隐私信息的综合保护框架,并通过实证对其效果进行了检验和评价;A. Sunyaev 等[22]通过分析和评价移动健康应用的隐私保护政策,发现其存在与 APP 关联弱、可用性差、不易理解等问题。此外从用户感知视角探析隐私问题引发的 APP 用户行为反应也逐渐成为研究热点[23-25],但在这些研究中,账号注销仅作为一种辅助手段和补救措施被提及而缺乏深入探讨。

我国的个人信息保护研究已开展十余年,取得了较为丰硕的成果,对新媒体环境下的信息隐私研究则主要关注隐私行为、隐私保护等方面[26]。例如王晗等[27]构建了一种引入可信第三方服务平台的网络隐私保护模型;沈洪洲等[28]调研并比较了国内 3 种移动社会化媒体隐私保护功能的可用性;田波等[29]则在广泛调研的基础上设计了用于评价移动 APP 的隐私信息泄露风险的指标体系;张玥等[30]运用扎根理论对医疗 APP 隐私政策的用户认知及影响因素展开了探究。但真正涉及账号注销机制的文献大多只是简单的新闻报道。

概言之,现有国内外研究在账号注销机制方面的探索依然处于空白。因此,本文旨在立足当前移动互联网环境的新形势与新变化,对用户账号注销问题的国内外法律制度、实践现状进行系统调查、梳理和分析,并在此基础上尝试进行制度框架的设计以填补相关研究空白,为完善用户账号注销机制提供参考。

2 移动互联网环境下用户账号注销的相关法律

公民对本人账号进行注销、要求 APP 服务商删除个人数据,这是数据主体对网络中个人信息享有支配、控制、处置的权利体现。我国虽尚无“注销权”的明确概念与界定,但已有一些相关法律制度规定隐含了对用户账号注销权利的认定。

欧盟的数据保护体制自 20 世纪 70 年代始,经历了漫长的发展过程[31],直至 2016 年 4 月通过了号称“史上最严数据监管法”[32]的《通用数据保护条例》(以下简称 GDPR),GDPR 在原有《数据保护指令》(95 指令)的基础上进行了升级和强化,具有覆盖范围广、统一性强、处罚严厉等特点,被视为网络安全与合规性融合的里程碑[33],其面向未来的设计理念对全世界的数据治理生态产生了深远影响[34]。GDPR 中与账号注销相关的权利条款表述完整全面,自生效以来也逐渐被 Google[35]、Microsoft[36]、Amazon[37]等世界科技和互联网巨头广泛接受并付诸实践,具有重要的参考价值。而美国由于立法传统、法律观念及社会环境的影响,隐含“被遗忘权”等相关权利的规定较为分散和模糊,多与隐私权并置,实施阻力和争议也较大,整体态度比较消极[38]。

因此我们主要对与账号注销相关的我国法律制度,以及欧盟 GDPR 的相关规定展开梳理,以为后文制度的比较和构建奠定基础。

2.1 我国的相关法律制度规定

如今网络账号包含的信息不但与用户个人密切相连,同时具有极高的商业价值和潜在利益,因此兼具人格权和财产权的权利属性。用户数据不仅是用户的虚拟财产,也是用户数据权利的集中体现,虽然我国法律现今尚未有个人数据权和“被遗忘权”等界定[39],但部分学者认为其可作为隐私权在数字时代的延伸[40]。因此我国的账户注销相关权利主要以隐私权和个人信息保护的相关条例作为法律基础,包括了直接保护和间接保护两类。

一类是直接保护。例如在 2012 年 12 月 28 日由人大常委会通过的《全国人民代表大会常务委员会关于加强网络信息保护的决定》[41]中,第一条就将“能够识别公民个人身份和涉及公民个人隐私的电子信息”纳入到国家的保护范围中,对于泄露个人身份、散布个人隐私、受商业性电子信息侵扰的情况,公民“有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止”。2017 年 6 月 1 日正式实施的《中华人民共和国网络安全法》,不但为我国的网络安全提供了多重保护,同时也进一步强调了用户自身对个人数据的控制权和决定权。其中 22 条、40 条、41 条、42 条、43 条等条款的规定对网络运营者的个人信息使用行为进

行了清晰的限定,其中明确指出运营商对个人信息使用的“目的、方式和范围”,需经被收集者同意;用户若发现运营商存在违法、违规使用其个人信息的行为,有权要求其删除个人信息等。这样的规定体现出用户应对个人数据信息有自主控制的权利,这一权利贯穿了个人数据产生到消亡的始终,依法删除个人信息是网络运营商应尽的义务。

另一类是间接保护。例如我国《宪法》第 38 条规定:公民的人格尊严不受侵犯;我国《刑法》也将非法获取或提供、出售个人信息量刑入罪;《侵权责任法》第 36 条规定:网络用户、网络服务提供者利用网络侵害他人民事权益的,应当承担侵权责任;《消费者权益保护法》第 29 条规定:经营者收集、使用消费者个人信息,应当遵循合法、正当、必要的原则……经营者应当采取技术措施和其他必要措施,确保信息安全,防止消费者个人信息泄露、丢失。

此外在部门规章层级,工业和信息化部颁布的《电信和互联网用户个人信息保护规定》中第二章第 9 条明确指出:电信业务经营者、互联网信息服务提供者在用户终止使用电信服务或者互联网信息服务后,应当停止对用户个人信息的收集和使用,并为用户提供注销号码或者账号的服务。

综上所述,虽然我国现有法律体系中还没有专门的个人隐私保护法,也没有与用户账号注销直接关联的明文规定,与之相关法律法规分布较为分散,内容相对简单,传统的隐私保护法律在当今移动互联网环境下有诸多不相适应的地方。但已有的法律规定表明在个人信息的采集和使用上,用户享有充分的知情权和决定权。同时,用户可依法要求网络平台停止使用和删除清理个人信息,以防范隐私泄露情况的发生。网络运营商不但应在法律框架内合理使用用户信息,还有义务提供账号注销的相关服务,在用户终止使用后及时停止对用户信息的挖掘和使用,以保障用户自主选择的权利,这也是在保护个人信息中包含的人格利益。

2.2 欧盟 GDPR 的相关规定

在移动互联网环境下,为帮助公民更好控制和处理个人信息,防止个人信息被过度采集和使用,欧盟在 2012 年率先正式提出了“被遗忘权”的概念[42],并在 2014 年“谷歌诉冈萨雷斯案”中首次在判决书中付诸实践,使其真正成为一项可操作的民事权利[43]。

1995 年,欧盟颁布的《个人数据保护指令》就已经能看到“被遗忘权”的影子,其中第 6 条第 1 款(e)项限定了数据的使用不得超出数据最初采集的目的,第 7 条对数据处理的具体情形做了限定,但 14 条认为公民可以拒绝以直接营销为目的的数据处理,另外第 12 条(b)项中明确指出在数据处于不完整或不准确的情况下,公民有权利“擦除与本指令规定处理不符合的数据”[44]。在此基础上,2012 年欧盟发布了 GDPR 的提案,以对“95 指令”的相关内容进行更新,其中最明显的变化就是对被遗忘权的权利主体、义务主体、行使条件等做了详细的规定。

经过数年讨论,欧盟委员会最终于 2016 年 4 月正式通过了 GDPR,以取代“95 指令”,该条例已于 2018 年 5 月 25 日起正式生效。从覆盖范围上看,依据该条例的规定,任何能够在欧盟境内被个人访问和使用的网络站点和手机 APP,都可以理解为“该产品、服务的目标用户包括欧盟境内用户”,即在此条例的适用范围之内,这意味着境外企业也不能免责。从义务主体上看,数据控制者还包括了传播信息的控制者,例如搜索引擎等,其不仅需要自身履行擦除义务,还有通知其他信息控制者的义务[43]。

根据 GDPR 的第 4 条规定,个人数据是“指一切与已识别或可识别的自然人(数据主体)相关信息”,姓名、身份证号、位置数据、网络标识符,甚至是自然人的身体、心理、遗传、文化、社会等各方面特征都囊括其中,可见其具有很强的覆盖性。

GDPR 的第 17 条为“擦除权(Right to erasure)”,并已将草案中分列的“被遗忘权(Right to be forgotten)”并入其中,该条例直接保障了用户注销的权利。据其第 1 条款规定,在数据被收集的目的已不再必要或被非法处理、用户撤回同意、依据成员国法律应当被擦除等情形下,用户数据应被立即删除,相关方面不得无故拖延。其第 2 条款则进一步指出,若控制者公开传播了符合 1 条款的个人数据,除了自己清除外,还应采取包括技术措施在内的相应手段,通知其他数据控制者,删除相应数据链接和复制件,即让第三方同时停止对个人数据的利用。其第 3 条款则规定了数据保留的一些特殊情况,包括数据遗忘不能阻碍他人的言论自由,也不能损害国家利益和公共利益等等。此外,第 21 条 2 款延续了“95 指令”的传统,认为用户可以拒绝个人数据被应用于直接的营销目的。GDPR 也对侵犯“被遗忘权”的行为制定了严厉的惩罚措施,根据第 83 条第 5 款,当数据控制者不能按照第 17 条的相关要求保护个人数据时,最高可被处以两千万欧元的行政罚款,或企业一年全球营业额 4% 的罚款。

GDPR 第 20 条则明确规定了数据主体应拥有数据的“可携带权(Right to data portability)”,能够帮助用户在账号注销前或注销时更好地转移数据。从适用范围上看,“可携带权”是针对在数据主体明确同意基于特定目的而授权控制者处理其个人数据的情况下,由数据主体提供给控制者的相关个人数据,以及在服务过程中通过自动方式形成的用户数据,但这类数据不包括从其他渠道所收集的数据和数据控制者进行二次挖掘所衍生的数据[45]。从数据形式上看,数据主体所获得的个人数据应是结构化、经过整理、机器可读且格式普遍的。从数据的使用目的上看,数据主体在得到此类数据后有权将其传输或迁移到另一控制者处。

此外 GDPR 还规定“可携带权”的行使不得影响第 17 条中“被遗忘权”的相关规定,且“可携带权”和“被遗忘权”均不适用于涉及控制者为了公共利益或行使官方权威授予的正式权利的数据处理行为,行使中也不能对他人的权利或自由、履行法律义务等产生负面影响。同时在某些特殊情况下部分特殊类型数据也可允许处理。此外 GDPR 在 18 条还确立了数据主体对控制者的“限制处理权(Right to restriction of processing)”,以对处理行为进行限制。

GDPR 是一部具有普适性、针对个人数据建立的保护法律,其不但对数据处理中的各种角色及其行为进行了详细界定和要求,同时着重强调和扩展了数据主体所具有的权利,尤其是数据控制者的相关行为应对其透明、经其同意。根据 GDPR 的条款,在法律允许的范围内,数据主体有权终止数据服务,并有权要求数据控制者、处理者删除数据或将数据返还,以切实保障个人的合法权益。现今随着 GDPR 开始生效,其深远影响正逐渐显现,这也意味着用户应该拥有注销账户的权利,并能够主动将自己的个人信息进行收回或删除。

3 国内外移动互联网 APP 用户账号注销机制比较

国内移动互联网环境下的隐私研究相较国外起步较晚[26],同时由于法律制度、政策体系、社会环境、历史文化[46]等不同因素的综合影响,国内外账号注销机制在 APP 的具体实践中也存在着较大差距,进行横向对比有利于发现问题,以进一步完善发展。同时,具备一定用户规模与稳定市场占有率的 APP 在注销机制上更具完备性、实用性与可靠性,其实施也将对相关主体产生更广泛和深远的影响。因此为增强研究结论的可推广性,我们参照苹果应用商店(APPLE APP STORE)2018 年 12 月中国和欧洲地区 APP 下载榜单前 100 强及各领域 TOP5 数据[47],于 2019 年 1 月分别选取了不同领域的 10 款用户数量在千万以上的 APP 开展调研。其中国内 APP 包括社交类的微信、QQ、微博,购物类的淘宝、京东,出行类的滴滴打车、摩拜单车,搜索类的百度,支付类的支付宝,知识类的知乎等;国外 APP 包括社交类的 Skype、Facebook、LinkedIn,购物类的 eBay、Amazon,出行类的 Airbnb、Uber,搜索类的 Google,支付类的 PayPal 等,并主要从注销前 APP 所获取的用户数据、注销时的前提与流程、注销后的数据保留情况等方面开展研究。根据上文 GDPR 的管辖范围规定,经查证所选 10 款国外 APP 既在欧盟地区有较高流行度,其相关政策也已响应 GDPR 的要求进行了调整。因此我们重点以欧盟用户的身份开展国外部分调研,以中国用户身份开展国内部分调研,以保证研究效度。具体结果汇总见表 1、表 2。

根据实践调查结果,我们可以从如下几个方面对国内外 APP 的注销现状进行比较与分析。

3.1 注册与注销的难易问题

从总体上看,国内 APP 账号呈现注册较容易、但注销较困难的情况。大部分 APP 注册流程十分简单,可通过第三方授权甚至是手机验证的方式快速完成注册。但在注销中,一部分服务商没有提供注销入口,甚至无法注销账号,另一部分服务商的注销入口相对隐蔽,不但注销渠道单一,同时注销限制及前提条款繁杂,尤其是社交类和购物类 APP。例如新浪微博注销需满足的要求多达 7 项,要求用户将微博账号“与其他 APP 网站的账号解绑”“清空站外授权关系”,但并没有为用户提供相应的授权列表或绑定列表。摩拜单车还要求提供“身份证原件”和“手持身份证照片”,以对用户身份进行确认。这些条件使得用户注销费时费力,阻碍重重。

而国外的账号注册与注销过程均相对简单。部分国外 APP 在首次使用时,除了常见的使用用户名、密码或邮箱、手机号外,也可直接通过其他用户规模较大的互联网平台账号,例如 Microsoft、Google 等,以授权方式登录。在注销时,国外服务商通常允许用户通过 APP 内置选项自行“删除账户”,注销过程相比国内简洁。Airbnb、eBay、LinkedIn 等 APP 只需勾选“注销原因”即可,备选原因通常包括“无法满足需求”“隐私安全考虑”等。部分授权互联网平台还提供了关联账号管理中心,例如 Google 允许用户快速删除 Gmail 或 YouTube 等指定服务。在用户提出注销申请后,社交

表 1 国内主流 APP 账号注销现状

名称	收集数据	能否主动注销	注销前提/条	注销途径	能否被动注销	注销清除的数据	可能保留的数据及年限	注销可否终止	注销的替代方案
QQ	①②③④⑧⑨⑩	√	4	无	√	个人资料、历史信息及授权服务记录	合理期限内删除全部信息与内容	√	冻结账户
微信	①②③⑧⑨⑩	√	4	APP 端	√	所有资料及授权服务记录	无说明	√	冻结账户
新浪微博	①②③④⑤⑥⑦⑧⑨⑩	√	7	APP 端 人工	√	用户发表内容	无说明	√	无说明
淘宝	①②③④⑤⑥⑧⑨	√	7	APP 端 Web 端	√	删除部分个人信息	有权继续保留"各类信息";订单信息	×	停用账户
京东	①②③⑤ ⑥⑦	√	8	APP 端 Web 端	√	账户信息交易记录授权记录	相关交易记录在后台保存 5 年甚至更长	√	锁定账号
滴滴	①②③④⑤⑦	√	4	APP 端	√	实名认证信息、行程信息、个人隐私信息	无说明	×	无说明
摩拜	①②③⑤	√	2	邮件	√	账号相关所有数据	保存部分信息	×	无说明
知乎	①②③⑥⑧	√		站内信 邮件	√	个人资料、UGC 内容付费产品记录等	已绑定的手机号、邮箱和第三方社交账号	×	无说明
百度	①②③⑤⑦	√	5	APP 端	√	个人信息;身份信息;第三方授权信息交易记录等	无说明	×	冻结账户
网易邮箱	①②⑦	×		无	√	所有信息和资料	无说明	×	无说明

注:"收集数据"一栏编号说明:①身份识别数据;②位置及行程数据;③联系方式数据;④第三方数据;⑤金融支付数据;⑥搜索浏览数据;⑦设备数据;⑧UGC 数据;⑨运动健康数据;⑩相册数据;⑪个人档案数据。下同

表 2 国外主流 APP 账号注销现状

名称	收集数据	能否主动注销	注销前提/条	途径	能否被动注销	注销清除的数据	可能保留的数据及年限	注销可否终止	注销的替代方案
Skype	①②③⑤⑦⑩	√	7	注销授权账号	√	所有产品和服务、个人文件	60 天	√	无说明
Facebook	①②③⑩	√	无	APP 端 Web 端	√	所有用户资料及用户所发表内容	最多 90 天	√	停用账户(可随时重新激活)
LinkedIn	①②③⑪	√	无	APP 端 Web 端	√	个人身份信息	最多 30 天	√	无说明
eBay	①②③⑤⑧	√	2	Web 端	√	所有资料及授权服务记录	关闭账户需要 30 – 60 天	√	延迟注销
Amazon	①②⑤⑪	√	3	邮件人工	√	所有资料及授权服务记录	无说明	×	停用账户
Airbnb	①②③④⑤⑦	√	无	App 端 Web 端	√	与他人分享的信息、地理信息	在必要时间段内保留部分个人信息	√	停用账户
Uber	①②③⑤⑦⑧⑩	√	无	App 端 Web 端	√	行程信息、增值信息、个人身份信息	保留部分人信息;其他数据将保留 30 天。	√	无说明
PayPal	①③④⑤⑦	√	1	Web 端	√	个人资料相关数据	保留部分信息	×	无说明
Google	①②③⑥⑦	√	1	APP 端 Web 端	√	账号所有信息数据,包括所绑定与授权服务的信息	保留部分信息。其他数据需要 2 – 6 个月彻底清除。	×	无说明
YouTube	①②③⑥⑧	×	1	注销授权账户	√	Google 账号相关所有数据	无说明	×	暂时隐藏或永久删除频道

类 APP 通常承诺将用户数据保留一定时长,Skype、Facebook、LinkedIn 都允许用户在此期间恢复或重启账户,期满后再执行数据封存或删除操作。

3.2 注销的主动权问题

从发起对象看,用户账号的注销方式大体分为两类,一类是用户主动进行注销,另一类是账号被服务商注销或封禁。在国内,注销的主动权掌握在 APP 服务商手中,用户的选择余地较小。各 APP 服务商在用户注册时的"服务协议"和"个人信息保护政策"中普遍将账号注销作为一种惩治用户违反协定或法律的重要措施。例如微信规定对于违反服务协定的用户腾讯有权做出"账号注销的处罚"。还有一些服务商设立了

账号回收机制，网易邮箱和百度均规定可回收连续6个月无操作的账号。可见服务商在账号注销上具有很大权限，但对于用户发起的注销申请，大部分公司在注册协议中没有明确的条款约定，如知乎、摩拜等APP还需联系人工客服申请和确认，服务商对是否准予注销有最终决定权和解释权，并能在国家机关调查等特殊情况下终止注销进程。

国外APP在服务和隐私条款中对用户注销账号权利的强调甚于国内，尤其是面向欧盟的GDPR法案做了相应调整和细致修改，强制注销则多在用户违反法律法规或条款政策的情况下触发。Amazon规定了用户查阅、更正、删除数据的权利，并提供了联系第三方服务争端解决机构、"隐私盾协议"工作小组的渠道，以帮助欧洲用户更好地实现数据主体权利。仅在违反"适用法律、条款、方针和政策"时，Amazon保有终止账号使用的权利。此外冻结或禁用账号也是国外APP服务商维护社区健康和服务安全、遵照政府部门指令的常用措施，以避免法律风险及责任，Facebook、Twitter等在遇到此类情况时会向用户发送冻结或禁用通知，允许用户根据提示进行申诉、解禁或其他操作。

3.3 注销后服务商对用户信息的保留及使用问题

国内APP普遍存在数据清除、留存和后续使用不透明的情况。各服务商均在隐私保护的相关条款中对APP获取的数据做了说明和规定，数据主要来源于用户主动提供、使用过程中产生和第三方授权这3类。调查中大部分APP一方面在服务协议中规定注销将清除"账户相关信息"，另一方面又指出将会保留部分信息一定时长。其中国内购物类APP较国外既在使用时获取更多种类数据，也在注销时保留更多用户信息。例如淘宝规定用户撤回同意"不会影响此前基于您的授权而开展的个人信息处理"，也"不会立即从备份系统中删除相应的信息"，意味着即使注销完成服务商也保留部分用户数据，"注销残留"问题广泛存在，仅对用户不可见的"假注销"时有发生。京东在《注销须知》里明确提到个人信息只在"前台系统去除"，"相关交易记录"可能在后台"保存5年甚至更长时间"，百度也"仍可保存用户注销前的相关信息"。"假注销"在以用户生成内容为核心要素的知识类APP中体现尤为明显，"知乎"账号注销后，用户发表内容不会完全删除，仍可被查看，仅显示账户为"封禁状态"，同时"已绑定的手机号、邮箱和第三方社交账号均不会自动解除绑定，并将不能用于申请新的知乎账号"，为用户的再次使用造成障碍。将敏感信息匿名处理是服务商宣称的常用措施，但其过程并不透明。服务商通常未明确告知用户注销后保留的数据类型、保留时长、使用目的等。

国外APP也存在类似问题，服务商在用户提出销户申请后，通常会声明附带影响、提醒数据能否恢复、后续可否再注册等，并给予一定时长的"后悔期"。但部分APP的注销仅是针对用户无法再次登录账号而言，服务商则可能将用户信息无限期保留在服务器和数据库中。另外一些服务商在数据保留上含糊其辞，如表述为"在商业合理的时间范围内保留用户信息和用户内容""在必要时间段内保留部分个人信息"，Facebook等提出在特殊情况下用户信息的访问和保留时间期限可能会被延长。与假注销的情况类似，除用户评论、用户消息外，还有一部分未注明的用户数据也可能会被服务商保留。Airbnb表示将"不会删除某些用户数据"，包括住宿评价、交流消息等，而是去除身份信息或解除关联，并长期留存。

3.4 面向用户的"数据可携带权"问题

对于用户数据，国内APP用户条款中服务商的权利大于义务。注册时服务商对数据进行最大限度地获取，而注销时仅规定了用户方的前提条件，对自身义务规范则无明确规定。与"假注销"情况相对应的是，APP服务商并没有尽到帮助用户保留和迁移数据的义务，用户无法通过服务商提供的相应渠道来有效、完整地保存个人数据到本地，如QQ要求注销用户"自行备份"。只有少数海外版APP，特别是供欧洲用户使用的版本拥有保障数据主体"可携带权"的条款和措施，允许用户通过主动联系服务商进行保留操作，但缺乏成熟处理体系。

对于用户信息的自留问题，大部分国外APP设计了较为完善的面向用户的信息保留机制，提供了包括UGC数据、个人资料、位置数据等账户数据在内的下载通道，并在注销过程中主动提醒用户更好地保存、调用和迁移在平台上所产生的数据信息，以防注销后无迹可寻。在Facebook的注销页面，用户可申请下载个人数据，包括所发推文、聊天记录、个人资料，甚至是点击广告、登录IP等；LinkedIn同样允许用户下载包含文章、联络人、通讯录、消息等所有个人信息；Uber以及Amazon等也提供了用户数据副本的专用获取通道。这些数据会被转换为不同格式的可机读文件并压缩打包以供用户在一定期限内完成下载。相较于国内搜索类APP百度，旗下同样拥有庞大产品群、账号关联复杂的Google规定更为明晰和科学，在注销账户前，用户

可下载 30 多项 Google 相关产品数据,完成归档后将通过电子邮件获得下载链接,并可在线管理归档文件。更为人性化的是 Google 允许用户制定“闲置账号处理方案”,以便在去世或停止使用时自动触发账户删除操作,或将账号相关内容和数据分享或发送给指定联系人。

3.5 注销中对第三方授权的处理问题

现今以“数据授权”方式进行注册的情况愈发普遍,国内微信、支付宝等用户基数大的授权平台面向第三方的数据接口众多,而在注销时却把清除责任推给用户,要求用户自行解除授权绑定,而没有履行帮助用户及时、彻底清除个人信息的义务。当注销操作在授权 APP 发起时,由于对已授权平台的信息处理缺乏相应规定,被授权 APP 能否同步清除用户数据、链接仍旧存疑,用户难以从服务商及第三方处彻底抹除和回收个人信息,遗留了信息泄漏和被恶意利用的隐患。

国外 APP 也可使用社交媒体平台账号直接登录,其中部分 APP 作为互联网巨头体系下的分支应用或服务,没有独立账号系统,如 Bing 只能使用 Microsoft 账号登录,它们在数据上属于“隶属关系”。当用户产生登录行为时,表示同意向分支应用授权,分支应用得以与原数据持有平台共享用户数据,并扮演“数据处理者”的角色。用户难以单独删除这些分支应用账户,需在授权账户进行操作。例如用户若想删除通过 Google 登录的 YouTube 账号,可在 Google 账户管理中心将对 YouTube 服务的授权取消,或将与之联通的 Google 账号一并注销。

国内处于扩展用户基数阶段的 APP 大多也提供了使用社交类 APP 账号登录的入口,但这些 APP 一般以第三方授权的方式获取用户信息,并进一步成为数据的实际控制者,即它们与授权 APP 在数据上属于“平级关系”。在用户使用社交媒体账号登录后,APP 将自动获取信息并创建“独立账号”,通常还要求用户二次绑定手机或邮箱等。在此情况下注销操作需在原 APP 和现 APP 分别进行,仅注销其中一方账户不代表解绑授权关系。因此若用户想彻底注销,需依次完成解绑第三方授权、分步注销等操作。

而国外 APP 对于处理注销中的“平级关系”表现出相对审慎和主动的态度,例如 Amazon 指出第三方对数据的使用也必须符合其制定的隐私保护义务,除非能够证明不对造成数据损害的事件负责,否则 Amazon 将对第三方的不作为承担责任,国内现今也有相似趋势。

3.6 注销条款及机制的地区差异

国内 APP 的注销条款在海内外版本上有所差异。支付宝、微信等国内主流 APP 在国际版服务条款中,均存在针对不同地区的特定条款。如“微信国际版”隐私政策根据欧洲法律明确规定了用户的账号注销权利、提供了删除数据申诉通道,不但对各类用户信息的处理方式及目的、注销后保留期限做了详细说明,还承诺将“停止处理个人信息”的消息“尽力告知”第三方等。支付宝海外版“Alipay”的隐私政策分为“全球版”和“欧盟版”,均明确用户能够申请删除个人信息。这些国外版条款遵循并适应属地法规,并且特定条款优先于通用条款。

国外注销条例的地区差异更为普遍。通过比较发现国外 APP 隐私条款也会针对服务所属国家和地区的法律进行与之相适的调整,或为特定地区用户提供特别服务,尤其是在 GDPR 法案推行的欧盟地区。如 Airbnb 依据所在地区将用户数据划归相应分公司管理,并进一步根据地域法律及规定采取差异方案及不同程度的管控。若用户更改所在地区,其数据将在不同区域的数据控制者中流转,并以此转移和变更服务关系,此时如提出注销申请,服务商即根据用户现所在地区的法律及政策履行相应义务。遵循 GDPR 的相关规定,欧洲地区用户可随时申请查看、更新、删除个人资料或账号,并要求 APP 在验明用户身份后及时给予回应和反馈。LinkedIn 等甚至为欧盟地区用户提供了彻底抹除平台中个人数据的特权通道。APP 服务商采取地区差异化的管理举措,一方面是为了符合不同国家的强制性要求,另一方面也使注销设置能满足各类用户的实际需要。

4 移动互联网环境下的全流程账号注销机制设计

综上可以发现,GDPR 从适用范围、数据擦除权、数据可携带权等方面,为保障用户账号注销构筑了坚实的法律基础,APP 注销现状已有所改观。但仍存在诸多不足,账号注销流程繁复、服务商权利大于义务、数据留存与使用不透明、注销后续机制不完善、第三方授权处理不彻底等问题持续困扰着用户。尤其是在中国,用户信息保护意识薄弱,信息滥用甚至是黑色数据产业更使用户信息安全面临巨大威胁。

让用户信息能够自由退出是解决当下困境的关键一步,也只有通过服务商、监管机构、用户三方协力,构建并完善覆盖用户信息全生命周期的账号注销机制,

才能真正规范数据处理行为，切实保障用户隐私安全，消除后顾之忧。本文认为账号注销机制是指在APP账号注销过程中，基于相应法律规定与技术标准，为解决信息用户面临的后续数据清除问题而构建的一整套规范化、模块化、流程化、总括性信息管理方案与数据处理体系，旨在应对信息退出瓶颈与情境、厘清多方主体权责与关联、保护用户信息权益及个人隐私。因此，从注销前、注销中、注销后这三个阶段入手，笔者借助GDPR的理念及实践，移动互联网环境下的全流程账号注销机制实现路径可依如下3个部分进行设计。

4.1　注销前的保障

账号注销的顺利进行必须以完善的制度规定作为基础。根据现阶段存在的问题，如图1所示，APP服务商的用户协议条款及隐私保护协定至少应该涵盖以下四方面内容：①APP在使用的不同阶段从用户方面获取的数据类型、范围、使用目的、应用方面和处理方法等；②服务商和用户双方在账号注销问题上的权利及义务，需遵守的相关规定；③用户注销的具体流程，以及注销后不同类型数据的处理方案、保留目的、保留时限等；④针对APP服务商对第三方处理者和控制者进行数据授权以及将数据转移到第三方的情况，所制定的保证多方数据处理一致性、帮助用户彻底注销账号的具体规定及措施。

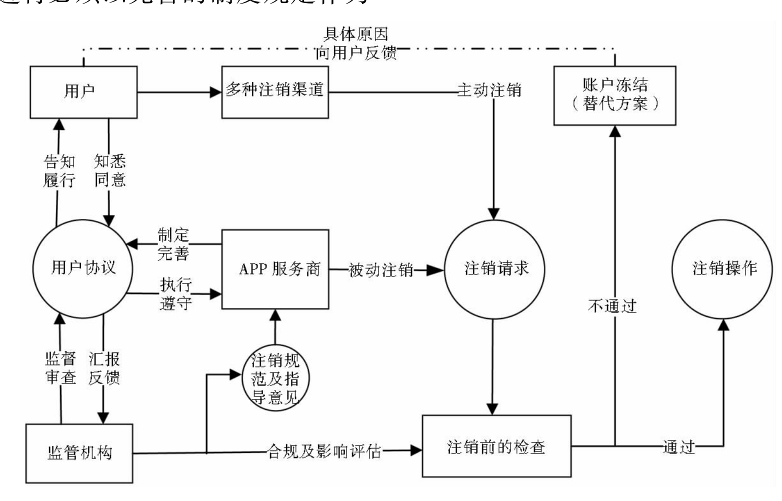


图1　注销前的保障路径设计

用户既需要在注册时仔细阅读、知悉并同意有关协议条款，还应养成良好的注销习惯，降低个人隐私泄露的风险。根据上文注销行为的不同发起主体，除用户不再使用相关平台、主动申请注销个人账号外，也应允许服务商根据相关法规制度，对危害平台安全或有不法行为的用户进行强制注销。在移动互联网环境下，服务商应为用户提供包括APP客户端、Web端、人工客服、邮件申请等在内的多种账号注销渠道，以保证用户注销申请顺利发起。

在收到注销请求、进入正式注销流程前，服务商应设置多层核验，既需要核实用户的身份信息、了解注销原因，还应根据不同领域APP的实际需要，遵循“最小必要原则”，按照最小限度设置必要的注销前提条件，避免恶意注销的发生。对于未通过核验的申请，及时向用户反馈具体原因，可推荐用户采用“冻结账号”的替代方案限制数据处理行为。

在这一阶段内，监管机构必须首先明确各类APP账号注销中对数据的处理方案，包括涉及的具体技术手段、处理情境与目的、处理方案与范围、处理时限等，将可能会对用户、企业和国家产生的具体影响，并综合评估其中的风险问题，从而发布针对不同领域APP的账号注销指导意见。其后通过对APP用户协议进行监督审查，以确保权利细则的准确性和具体条款的合理性，帮助APP服务商更科学规范地构建账号注销制度。

4.2　注销中的处理

注销处理主要围绕服务商展开，服务商掌握的数据不但包括用户“主动”提供的数据，还包括用户在使用过程中“被动”产生的用户画像及第三方授权数据等，这些信息从多维度刻画了用户本体及其行为。因此如图2所示，作为账号注销体系的实施主体，在注销操作中服务商首先需要面向以下三方面制定注销计划。

（1）面向用户的数据留存机制。APP服务商应该允许用户行使“数据携带权”，主动提醒用户在进行注销前有选择地拷贝或备份APP平台中的个人数据，并

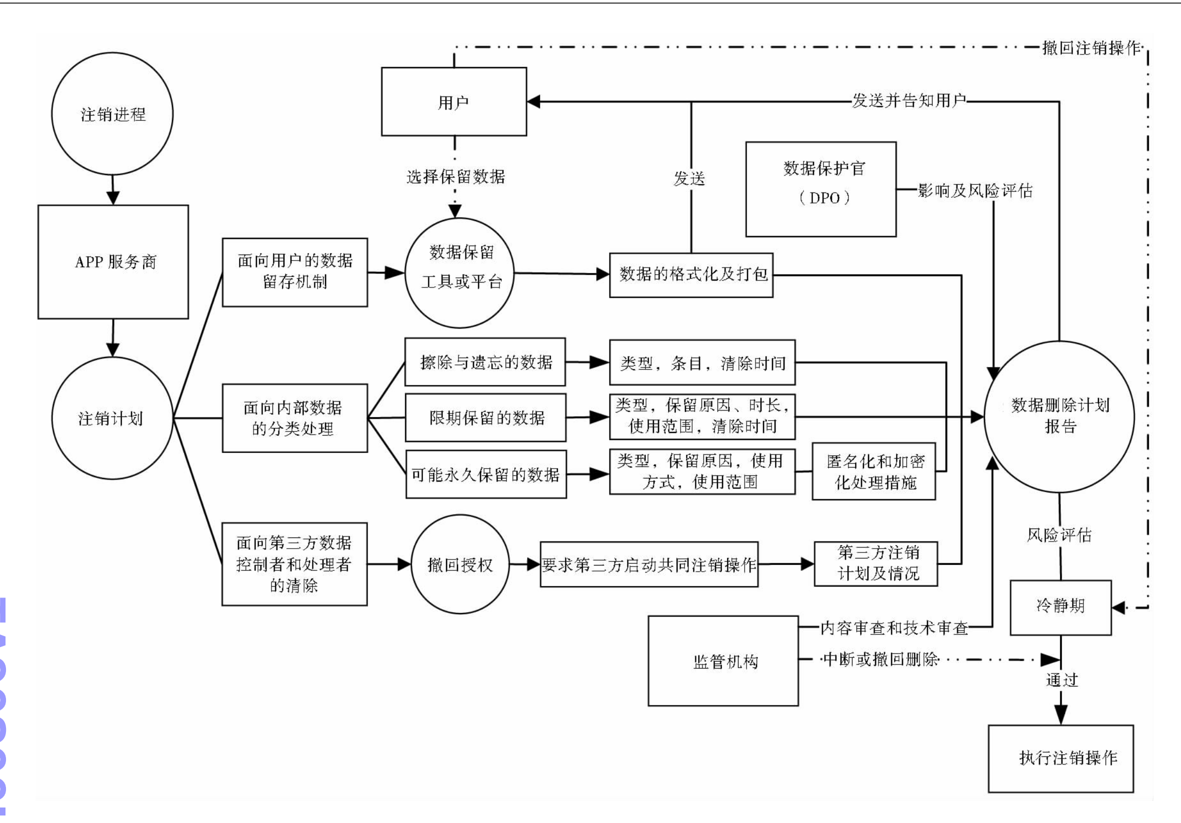


图 2 注销中的处理路径设计

提供便于用户保存、传递、迁移、再利用的获取渠道和文件格式，可考虑设计相关工具帮助用户自定义地将数据下载到本地，以保障用户无障碍地将机器可读的数据在不同服务商之间迁移的权利。

（2）面向内部数据的分类处理机制。根据监管机构的指导意见以及"数据最小化"原则，服务商对于不同类型数据的处理方式应主要分为 3 种：一是彻底擦除和遗忘，大部分用户数据应当永久性地从服务商的服务器和数据库中清除，并向用户报告相应类型和清除截止时间。二是限期保留，由于国家安全和企业需要、数据稳定性要求等原因，少部分数据可由服务商在一定期限内保留，但需向用户反馈保留数据的类型、原因、使用范围、保留期限、清除时间等。三是永久保留，极小部分数据可由服务商永久保留，除了向用户提供相应信息外，这类数据还需要进行严格的匿名化处理，包括对部分字段进行删除、替代、屏蔽，随机加入无意义信息，对身份识别信息进行不可逆的加密、去标识化等手段。

（3）面向第三方数据控制者和处理者的清除响应机制。对于使用过程中经用户同意，服务商将用户信息交由第三方处理并保存的情况，应将所有的数据授权关联明细告知用户，并允许用户保留或撤回授权。同时授权方应当通过技术化和自动化措施，及时知会第三方数据主体要求删除所保留的与用户数据有关的内容、链接等备份的信息，并请求其做出操作响应和结果反馈，帮助用户完成数据删除。

综合以上环节，服务商应向用户提供一份个人数据删除计划报告，同时给予来自企业内部数据保护官的法律风险提示与建议[48]，为用户设置一定时长的冷静期，允许用户在这一阶段内撤回账号注销申请并保留账号，若用户无反馈，则最终按计划执行账号注销及相应数据清除操作。注销流程及评估在某一 APP 中具有极强的可重复性，因此应在实践中固化为具体制度，并根据实际情况不断优化调整。

监管机构一方面必须监督服务商是否按照法律要求对用户数据进行合乎规范的处理，同时要根据数据删除计划报告，对具体删除、保留流程及结果进行审查，防止信息滥用和非法转移。另一方面当发现执行处理中的数据为危害国家稳定、公共安全或是处于行政司法机关调查中的数据，有权终止非法的账号注销操作，并对相应数据予以保留和冻结。

4.3 注销后的保护

在完成实际操作后，服务商应在一定时限内，据实制作特殊格式的用户账号注销处理结果报告，以保证报告可作为有关证据使用[49]。报告内容除了对服务商数据处理和保障措施的实施记录外，还应一并包含来自第

三方数据控制者和处理者的处理反馈，同时数据保护官应清晰明确地告知用户在注销完成后还可能存在的风险及法律问题，在有条件的情况下，可提供联系方式以便用户咨询及寻求帮助。最后服务商通过电子邮件等渠道将完整的注销处理结果报告发送给用户，并进行存档。

如图3所示，除了服务商本身外，数据保护官和监管机构需发挥更大作用，三方共同构成保护用户信息安全的责任闭环。数据保护官由企业委任、对企业负责，兼具专业的数据保护、信息安全法律知识和行业规范知识，能够从企业出发对账户注销的影响和风险进行评估，并提供专业化咨询服务，全方位地参与到账号注销的操作流程中，帮助企业构建注销体系、开展人员及制度培训、对相关风险进行评定并给予建议，同时应该成为沟通服务商和监管机构的纽带。

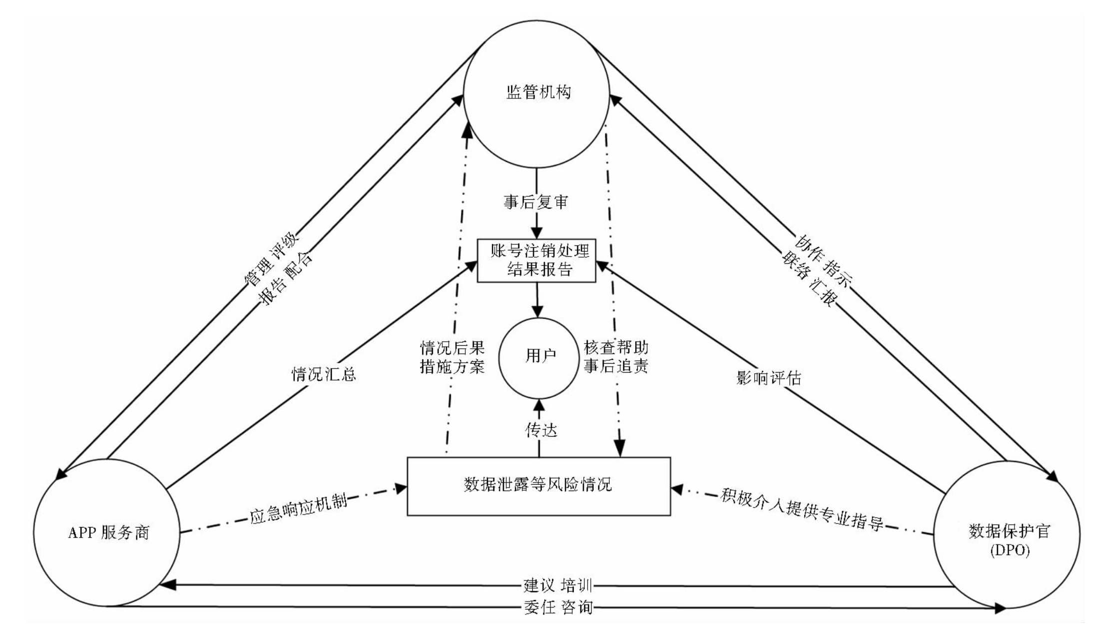


图3 注销后的保护路径设计

监管机构则需根据有关法律条例的规定，对照计划报告和结果报告，在事后对数据处理的合法性和妥当性进行复核，运用强制和非强制性结合的手段，对数据控制者和处理者的不当行为进行规制和矫正，敦促服务商进行整改或重启注销流程。同时监管机构应构建动态监管机制，要求服务商定期进行专项汇报，及时捕捉和识别数据处理过程中新的风险变化，从而达到持续化和常态化的监管目的，并根据相关实施情况提供指导性意见。

数据保护官应与监管机构保持密切合作，定期向监管机构汇报企业注销管理情况，接收监管机构的指示与要求。二者分别从内外两方面协作完成不同层级的风险评估和处理工作，审查和评估并不针对每一份用户注销申请，而是对某种数据或某类用户、某项操作的整体评估，从而减少各方的执行成本，提高执行效率。

当出现数据泄露等安全风险情况，尤其涉及账号注销后服务商依旧保留的、具有个人识别信息的数据处于泄露境况时，数据处理者和控制者应在指定时限内启动应急响应机制，向监管机构报告有关事实并告知用户主体，数据保护官应迅速介入评估情况、提供专业性建议，充分发挥风险管控的作用[48]，监管机构也应该及时指导救济行动，核实服务商是否严格遵守相关规定，并在事后启动追责和处罚机制。

此外监管机构可定期对服务商注销处理的技术性及组织性环节进行评级，基于流程的合规性、制度的完善性、人员的专业性、注销的及时性等方面进行相应的级别认证，通过公开信息及时向社会发布。

5 思考

聚焦于GDPR的实施，我们对国内外移动互联网APP的注销机制开展了系统调研，在理论结合实践的基础上，探索了账号注销机制的构建路径。目前由于服务商操作的不透明、用户注销意识不强、有关机构对个人数据的保护力度不足等原因，我国的账号注销机制还很不完善，甚至处于监管的真空地带，但这也恰恰为构建完善、周密、可行、实用的多级制度体系提供了契机。

用户数据在APP中的产生、存储、分析、利用、删除和保留是密不可分的连续过程，以用户为核心的保护也应一以贯之。因此要实现信息退出的规范化和常态化，保障用户的知情权和隐私权，需要政府机构、服

务商、数据保护官和用户等多方协调与配合,共同建立覆盖用户信息流完整生命周期的管理、保护、监督机制。尤其对于监管机构来说,在制度构建层面需加强顶层设计和标准建设,将账号注销作为制度构成的一个组件来处理,使其与信息流的其它监督、管理阶段相辅相成;在机构组织层面应建立如 GDPR 所述的独立、适当的多级管理体制,确立领导性监管机构的管理主位,负责指导、统筹和跨国背景下的协调,不同级别尤其基层监管机构也要因地制宜地开展工作,同时将第三方社会力量作为补充的监管要素,避免监管主体的缺位[49],使监管法律政策及制度体系具备良好的连贯性与适用性。

在 APP 的数据授权实践中,由相对权威平台经用户同意对第三方进行信息授权的模式可考虑进一步发展和完善。我国可引入如 GDPR 法案中界定的数据"控制者"和"处理者"的不同角色,由经监管机构权威认证的管理平台作为用户数据的实际控制者,通过规范的授权流程向作为"数据处理者"的 APP 提供数据,这些 APP 仅能最小化地保留用户数据。用户在数据管理平台中即可进行授权管理和账号注销,具体操作则由管理平台代行。这不但便于用户管理数据,也使得对数据的利用、监管更加高效。当然这其中的权责、监管以及数据垄断等问题仍有待深入权衡与研究。

此外随着手机存储空间和处理器的不断升级,还可以鼓励和支持 APP 对用户数据使用本地化的处理方式,依靠移动端的自身资源来完成信息的存储和处理,对服务端上传保存的数据尽量使用匿名化方式,从而削减账号注销的难度和复杂度,更好地保障用户的数据安全和退出权利。

参考文献:

[1] HASHEM I A T, YAOOOB I, ANUAR N B, et al. The rise of "big data" on cloud computing: review and open research issues[J]. Information systems, 2015, 47: 98-115.

[2] LUTZ C, HOFFMANN C P, BUCHER E, et al. The role of privacy concerns in the sharing economy[J]. Information, communication & society, 2018, 21(10): 1472-1492.

[3] 央视新闻. 评论:谁说"中国人愿意用隐私换便利"[EB/OL]. [2018-12-28]. http://news.163.com/18/0328/03/DDV513QI0001875N.html.

[4] 知乎. 如何评价京东杀熟? [EB/OL]. [2018-12-28]. https://www.zhihu.com/question/270660676.

[5] GU J, XU Y C, XU H, et al. Privacy concerns for mobile app download: an elaboration likelihood model perspective[J]. Decision support systems, 2017, 94: 19-28.

[6] JUNG Y, PARK J. An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services[J]. International journal of information management, 2018, 43: 15-24.

[7] WOTTRICH V M, VAN REIJMERSDAL E A, SMIT E G. The privacy trade-off for mobile app downloads: the roles of app value, intrusiveness, and privacy concerns[J]. Decision support systems, 2018, 106: 44-52.

[8] Backgroud checks. A directory of direct links to delete your account from web services[EB/OL]. [2018-12-28]. https://backgroundchecks.org/justdeleteme/.

[9] BRANDTZAEG P B, PULTIER A, MOEN G M. Losing control to data-hungry apps: a mixed-methods approach to mobile app privacy [J/OL]. Social science computer review, 2018: 1-23. [2019-04-29]. https://doi.org/10.1177/0894439318777706.

[10] DEVMANE M A, RANA N K. Privacy issues in online social networks[J]. International journal of computer applications, 2012, 41(13): 5-8.

[11] HERRMANN D, LINDEMANN J. Obtaining personal data and asking for erasure: do app vendors and website owners honour your privacy rights? [EB/OL]. [2019-04-29]. https://arxiv.org/abs/1602.01804.

[12] BAUMER E P S, ADAMS P, KHOVANSKAYA V D, et al. Limiting, leaving, and (re) lapsing: an exploration of Facebook non-use practices and experiences[C]//Proceedings of the SIGCHI conference on human factors in computing systems. New York: ACM, 2013: 3257-3266.

[13] LOCASTO M E, MASSIMI M, DEPASQUALE P J. Security and privacy considerations in digital death[C]//Proceedings of the 2011 new security paradigms workshop. New York: ACM, 2011: 1-10.

[14] EU. General data protection regulation[EB/OL]. [2018-12-29]. https://gdpr-info.eu/art-20-gdpr/.

[15] POLITOU E, ALEPIS E, PATSAKIS C. Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions[J]. Journal of cybersecurity, 2018, 4(1): 1-20.

[16] 中国消费者协会. 100 款 App 个人信息收集与隐私政策测评报告[EB/OL]. [2018-12-28]. http://www.cca.org.cn/jmxf/detail/28310.html? tdsourcetag=s_pctim_aiomsg.

[17] 信息通信管理局. 工业和信息化部信息通信管理局就加强用户个人信息保护约谈相关企业[EB/OL]. [2018-12-28]. http://www.miit.gov.cn/n1146290/n4388791/c6010832/content.html.

[18] 央视新闻. 手机 APP 账户难注销 工信部:需提供注销服务[EB/OL]. [2018-12-29]. http://www.xinhuanet.com/tech/2018-01/05/c_1122213028.htm.

[19] 工业和信息化部. 工业和信息化部关于电信服务质量的通告(2018年第4号)[EB/OL]. [2018-12-28]. http://www.miit.gov.cn/n1146295/n1652858/n1652930/n4509627/c6471882/content.html.

[20] ANTIGNAC T, SCANDARIATO R, SCHNEIDER G. A privacy-aware conceptual model for handling personal data[C]//International symposium on leveraging applications of formal methods.

Cham: Springer International Publishing, 2016: 942－957.
[21] FAWAZ K, SHIN K G. Location privacy protection for smartphone users[C]//Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. New York: ACM, 2014: 239－250.
[22] SUNYAEV A, DEHLING T, TAYLOR P L, et al. Availability and quality of mobile health app privacy policies[J]. Journal of the American Medical Informatics Association, 2014, 22(e1): e28－e33.
[23] KOKOLAKIS S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon[J]. Computers & security, 2017, 64: 122－134.
[24] GOLBECK J, MAURIELLO M. User perception of Facebook app data access: a comparison of methods and privacy concerns[J/OL]. [2019－05－13]. https://doi.org/10.3390/fi8020009.
[25] CHOI B C F, LAND L. The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage[J]. Information & management, 2016, 53(7): 868－877.
[26] 王晰巍,相甍甍,张长亮,等. 新媒体环境下信息隐私国内外研究动态及发展趋势[J]. 图书情报工作, 2017, 61(15): 6－14.
[27] 王晗,张玲. 面向个人信息管理的网络隐私保护模型研究[J]. 情报科学, 2015, 33(10): 47－51.
[28] 沈洪洲,汤雪婷,周莹. 我国移动社会化媒体隐私保护功能的可用性研究[J]. 图书情报工作, 2017, 61(4): 23－30.
[29] 田波,郑羽莎,刘鹏远,等. 移动 APP 用户隐私信息泄露风险评价指标及实证研究[J]. 图书情报工作, 2018, 62(19): 101－110.
[30] 张玥,王坚,朱庆华. 医疗问诊 APP 隐私政策的认知影响因素框架模型研究——基于扎根理论方法[J/OL]. [2019－05－17]. http://kns.cnki.net/kcms/detail/11.1762.G3.20190122.1424.004.html.
[31] 张里安,韩旭至. “被遗忘权”:大数据时代下的新问题[J]. 河北法学, 2017, 35(3): 35－51.
[32] 畅旎. 欧盟《通用数据保护法案》的影响与对策[J]. 中国信息安全, 2017(7): 90－93.
[33] ZERLANG J. GDPR: a milestone in convergence for cyber-security and compliance[J]. Network security, 2017, 2017(6): 8－11.
[34] 吴沈括. 欧盟《一般数据保护条例》(GDPR)与中国应对[J]. 信息安全与通信保密, 2018(6): 13－16.
[35] Google. We are committed to complying with applicable data protection laws[EB/OL]. [2018－12－08]. https://privacy.google.com/businesses/compliance/.
[36] Microsoft. Safeguard individual privacy with the Microsoft Cloud [EB/OL]. [2018－12－08]. https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview.
[37] Amazon. General data protection regulation (GDPR) center[EB/OL]. [2018－12－08]. https://aws.amazon.com/cn/compliance/gdpr-center/.
[38] 于向花. 被遗忘权研究[D]. 长春: 吉林大学, 2018.
[39] 周丹. 大数据时代个人数据民法保护问题研究[D]. 武汉: 华中师范大学, 2015.
[40] 李汶龙. 大数据时代的隐私保护与被遗忘权[D]. 北京: 中国政法大学, 2015.
[41] 新华社. 全国人大常委会关于加强网络信息保护的决定[EB/OL]. [2018－12－28]. http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm.
[42] REDING V. The EU data protection reform 2012: making Europe the standard setter for modern data protection rules in the digital age[C]//USA: Innovation conference digital, life, design munich. 2012, 22.
[43] 胡旭. 论被遗忘权制度的法律构建[D]. 武汉: 华中师范大学, 2017.
[44] 杨立新, 韩煦. 被遗忘权的中国本土化及法律适用[J]. 法律适用, 2015(2): 24－34.
[45] 曹亚廷. 数据可携带权及其对征信业影响初探[J]. 征信, 2016, 34(9): 26－28.
[46] COCKCROFT S, REKKER S. The relationship between culture and information privacy policy[J]. Electronic markets, 2016, 26(1): 55－72.
[47] Apple. APP store 排行榜[EB/OL]. [2018－12－09]. https://www.apple.com/itunes/charts/free-apps/.
[48] 宛玲. 国外个人数据保护官的概念、职责与能力素质[J]. 图书情报工作, 2018, 62(17): 129－135.
[49] 肖冬梅,谭礼格. 欧盟数据保护影响评估制度及其启示[J]. 中国图书馆学报, 2018, 44(5): 76－86.

作者贡献说明：

吴任力:提出论文研究框架,撰写、修改论文,设计注销机制;

吴淑倩:搜集资料及英文内容翻译,撰写论文,绘制注销机制图。

Research on User Account Cancellation Mechanism Under the Environment of Mobile Internet

Wu Renli[1]　NG Shuksin[2]

[1] School of Information Management, Wuhan University, Wuhan 430072

[2] Business School, The Chinese University of Hong Kong, Hong Kong 999077

Abstract: [**Purpose/significance**] Under the environment of Mobile Internet, service providers of APPs master an increasing amount of user data. Closing accounts has become an effective approach for users to prevent illegal use of indi-

vidual information. The construction of account cancellation mechanism is of great significance to guarantee users' information security. [**Method/process**] Based on the systematic investigations on relevant laws and regulations of China, and the General Data Protection Regulation (GDPR) enacted by EU, we have achieved a comprehensive understanding of status and problems of account cancellation mechanisms in popular APPs at home and abroad, then we proposed feasible construction strategies corresponding to the problems. [**Result/conclusion**] This paper proposed a whole-flow cancellation mechanism of user accounts, which covers three stages of account closing (i. e. before, during and after the process), implemented jointly by service providers, regulators and users. Moreover, we pointed out the direction of breakthrough and innovation in terms of managing and servicing users' information security in the future.

Keywords: the right to be forgotten personal data information protection data deletion data protection impact assessment